UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,596	01/15/2004	Christopher Newell Toomey	AOL0133	8695

22862 7590 10/20/2008

GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
10/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/759,596	TOOMEY, CHRISTOPHER NEWELL	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,5,8-10,12-16,19-38,41,42,45-47,49-53,56-86 and 89-94* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,5,8-10,12-16,19-38,41,42,45-47,49-53,56-86 and 89-94* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 2-3, 6-7, 11, 17-18, 39-40, 43-44, 48, 54-55, & 87-88 are cancelled. Applicant's arguments/amendments with respect to pending claims 1, 4-5, 8-10, 12-16, 19-38, 41-42, 45-47, 49-53, 56-86, & 89-94 filed 6/26/2008 have been fully considered but are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

Applicants contend "Shewchuk has nothing to do with issue of a trust token to a client by a server, and inclusion of a client identifier by the server in the token issued to the client by the server." Examiner would like to point out that Shewchuk et al. teach a trust token comprising a data object that includes a client identifier (par. 65-66). Furthermore, Examiner would like to note that Shewchuk et al. was introduced in order to suggest that a data object within a trust token can include a client identifier and that including the client identifier in the data object aids in strengthening the authentication step. Finally, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Applicants further contend that Crane et al. fail to teach/suggest "storing said issued trust token on said client." Examiner respectfully disagrees. Crane et al. teach that once a user is

authorized, i.e. deemed trustworthy, the authentication token is returned to the client (col. 5, lines 40-43). Furthermore, Crane et al. teach that the authentication token is used in order gain access/be authenticated to various devices within the framework (col. 5, lines 44-55). Thus, Crane et al. teach storing said issued trust token on said client.

Applicants further contend that Shewchuk et al. fail to teach/suggest "transmitting said stored issued trust token along with said user ID, authentication credentials, and client identifier from said client to said network service. Examiner respectfully disagrees. Shewchuk et al. teach that in order for a user to gain access to a network service, that user must submit a user ID, in addition to the security token assigned to the client to show it is trusted (par. 35-38 and par. 89). Since Shewchuk et al. was used to modify Crane et al., who teach that trust tokens are assigned to authorized clients, the combination of the two teach transmitting said stored issued trust token along with said user ID, authentication credentials and client identifier from said client to said network service.

Applicants further contend that "there is no teaching or suggestion in Okamoto of updating a database record contain at least…a date/timestamp of first and/or the current successful authentication." Examiner respectfully disagrees. First, Examiner would like to point out that the limitation in the claim calls for "adding or updating a database record containing at least..." Okamoto et al. teach a session data storage unit containing a user ID, network address, session ID, session key, and a valid period (col. 13, line 55 - col. 14, line 3). Furthermore, Okamoto et al. teach that the valid period is a time period in which a session is valid (col. 14, line 26) and may be set in such a way that it is a number of hours from the current time of the beginning of the session, i.e. date/timestamp of the first and/or current successful authentication

(col. 15, lines 1-8 and col. 26, lines 26-29). Therefore, Okamoto et al. teach adding/updating a database record containing at least…a date/timestamp of first and/or current successful authentication.

Applicants further contend that "there is no teaching or suggestion in the cited portions of Okamoto of using the user identifier to as a preliminary criterion for extending trust." Examiner respectfully disagrees. The limitation calls for "where the user identifier of a subsequent request matches that of a successful authentication, extending trust to the subsequent request if its originating network address and timestamp information satisfy predetermined criteria in relation to said record." Okamoto et al. teach that a user, having a user id, is entitled to successful continuous access when subsequent authentication requests are submitted if the requests are within the valid time period set forth in a previous access attempt (col. 15, line 60 – col. 16, line 4 and col. 16, lines 44-60). Furthermore, trust is extended to that entity based on the user ID (col. 20, line 66 - col. 21, line 8) and based on the originating network address (col. 10, lines 42-60 and col. 22, lines 20-49). Therefore, Okamoto et al. teach using the user identifier to as a preliminary criterion for extending trust.

Finally, Applicants contend that "there is no mention whatsoever in the cited teaching from Malan of adding response latency to untrusted logins." Examiner respectfully disagrees. Malan et al. teach a second policy for dealing with untrusted logins where various entities that seem to have malicious intent towards the system are considered to be untrustworthy (par. 67-68). Based on a determination that a host is not trusted, Malan et al. teach that the requests of those untrusted entities are subjected to rate-limiting procedures (par. 69). Applicants seem to disagree with the notion that malicious hosts are being interpreted as untrusted, however

Examiner would like to note that the claims are given the broadest reasonable interpretation according to MPEP 2111. Since the claims do not specify what constitutes a host being untrusted (other than the fact that it is not trusted), a malicious host is interpreted as being equivalent to that of an untrusted host. Thus, the combination of Malan et al. with Okamoto et al. teaches/suggests adding response latency to untrusted logins.

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. The prior arts of records taken singly and/or in combination teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 4-5, 8, 12-16, 19-28, 30-31, 35, 38, 41-42, 45, 49-53, 56-65, 67-68, and 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crane et al., US Patent No. 6,510,236 and further in view of Shewchuk et al., US Pub. No. 2004/0139352.

As per claims 1 and 38:

Crane et al. substantially teach a method/computer program product on a computer readable medium, comprising the steps of: identifying entities legitimately entitled to service, wherein an entity comprises a user ID-client pair, said user id-client pair comprising an individual user-machine combination (col. 3, lines 50-52); establishing said identified entities as trusted entities by issuing a trust token for each entity successfully authenticating to said network service, said trust token comprising a data object (col. 4, lines 5-10); said client identifier comprising at least one item of data that can be used to uniquely identify the client machine, wherein a user ID-client pair represents a unique entity (col. 4, lines 58-62); storing said issued trust token on said client (col. 5, lines 40-55); processing requests from said trusted entities according to a first policy (col. 3, line 61 - col. 4, line 10); and processing remaining requests according to at least a second policy (col. 3, line 54 - col. 4, line 10).

Not explicitly disclosed is the trust token comprising a data object that includes a client identifier. However, Shewchuk et al. teach that a credentials database containing client tokens is maintained in order to aid the system in an authentication step (par. 65). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to include the client identifier within the trust token. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Shewchuk et al. suggest that using a client token (which identifies the client) is useful in authenticating an entity in par. 66.

Also not explicitly disclosed is transmitting said stored issued trust token along with said user ID, authentication credentials, and client identifier from said client to said network service. However, Shewchuk et al. teach that a credentials database containing client tokens is

maintained in order to aid the system in an authentication step (par. 65). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to utilize the issued trust token, user id, and client id in order to gain access to various network services. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Shewchuk et al. suggest that using a client id, user id, and a trusted token provide a good amount of information which can be used to indicate that the client is trusted to gain access to various network services in par. 35-38 and par. 89.

As per claims 4 and 41:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 1 and 39. Furthermore, Crane et al. teach wherein entities legitimately entitled to service comprise entities previously able to successfully authenticate to a network service (col. 5, lines 1-6).

As per claims 5 and 42:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 4 and 41. Furthermore, Crane et al. teach wherein said network service comprises a server (col. 5, lines 14-27).

As per claims 8 and 45:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 1 and 38. Furthermore, Crane et al. teach said data object including: said user ID or a derivative thereof (col. 5, lines 40-43).

As per claims 12 and 49:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 11 and 38. Furthermore, Crane et al. teach said client identifier comprising any of: a client identifier assigned by said network service; and a client identifier provided by the client (col. 4, lines 49-63).

As per claims 13 and 50:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 7 and 45. Furthermore, Crane et al. teach further comprising a step of encrypting said trust token (col. 5, lines 40-43).

As per claims 14 and 51:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claim 13 and 50. Furthermore, Crane et al. teach further comprising the step of: transmitting said trust token from said network service to said client upon successful authentication to said network service by said entity (col. 5, lines 40-43).

As per claims 15 and 52:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 14 and 51. Furthermore, Crane et al. teach wherein said step of transmitting said trust token occurs via a secure channel (col. 5, lines 22-27).

As per claims 21 and 58:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 12 and 50. Furthermore, Crane et al. teach further comprising a step of storing said issued trust token in a server side database, indexed

according to a combination of user ID and client identifier (col. 5, lines 28-43).

As per claims 22 and 59:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 21 and 58. Furthermore, Crane et al. teach further comprising the step of: transmitting said client identifier assigned by said network service from said network service to said client upon successful authentication to said network service by said entity (col. 5, lines 28-43).

As per claims 23 and 60:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 22 and 59. Furthermore, Crane et al. teach wherein said step of transmitting said client identifier assigned by said network service occurs via a secure channel (col. 5, lines 22-27).

As per claims 25 and 62:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 21 and 58. Furthermore, Shewchuk et al. teach the method/ computer program product on a computer readable medium further comprising the steps of: transmitting said user ID and client identifier to said server; and retrieving said stored trust token from said database (par. 89).

As per claims 26 and 63:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 21 and 58. Furthermore, Crane et al. teach

wherein said server side database serves a plurality of services (col. 5, lines 44-55).

As per claims 27 and 64:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 2 and 40. Not explicitly disclosed is wherein processing requests from said trusted entities according to a first policy comprises the steps of: validating said trust token (par. 88-89); and processing request without adding incremental response latency (par. 89).

As per claims 28 and 65:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 27 and 64. Furthermore, Shewchuk et al. teach wherein said step of validating said trust token comprises the step of: verifying that the user ID and a client identifier in the trust token match those presented by the client on the request (par. 88-89).

As per claims 35 and 72:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 1 and 39. Furthermore, Crane et al. teach wherein said policies are applied by a server (col. 5, lines 44-55).

III. Claims 9 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crane et al., US Patent No. 6,510,236 and Shewchuk et al., US Pub. No. 2004/0139352 as applied to claims 8 and 45 above, and further in view of Morkel, US Patent No. 2002/0052921.

As per claims 9 and 46:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 8 and 45. Not explicitly disclosed is wherein said derivative comprises a cryptographic hash of the user ID. However, Morkel teaches that in order to maintain a secure id, it is hashed before being stored. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to hash the user ID in order to maintain security. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Morkel suggests that using a hash of the user's id secures the id from being compromised in par. 7.

IV. Claims 10, 29, 37, 47, 66, are 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crane et al., US Patent No., 6,510,236 and Shewchuk et al., US Pub. No. 2004/0139352 as applied to claims 6, 8, 28, 38, 45, and 65 above, and further in view of Pallante, US Pub. No. 2003/0028495.

As per claims 10 and 47:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 8 and 45. Not explicitly disclosed is wherein said data object further includes any of: a time stamp of first authentication to said network service by said entity; and a time stamp of a most recent authentication to said network service by said entity. However, Pallante teaches that logs are kept with timestamps of when users were authenticated in order to access documents. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to maintain a time stamp for a first and most recent authentication when the entity accesses the

system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that time-stamping and maintaining a log with the time-stamping information is important in non-repudiation proofs in par 154.

As per claims 29 and 66:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 28 and 65. Not explicitly disclosed is wherein said step of validating said trust token further comprises any of the steps of: verifying that a time stamp of a first authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable first-authentication time stamp; and verifying that a time stamp of a last authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable last-authentication time stamp. However, Pallante teaches wherein the token is a certificate which holds a validity period of when the entity can gain access to the system. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to enhance the security of the system by using a certificate instead of a password as the trust token and to allow access based on the validity period as defined by the certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that using a certificate and abiding by the validity periods in important to ensure that entities do not gain access unless they are allowed based on their privileges in par. 99.

As per claims 37 and 74:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 6 and 38. Not explicitly disclosed is further comprising the step of: updating said trust token after a login by a trusted entity. However, Pallante teaches that the trusted token may be a certificate in order to increase security, as well as renewing certificates when appropriate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to use a certificate as the trust token and to renew it when necessary. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that renewing a certificate will further ensure that appropriate entities gain access to resources for the full duration of the amount of time they are entitled to do so in par. 51.

V. Claims 16, 19-20, 24, 53, 56-57, and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crane et al., US Patent No., 6,510,236 and Shewchuk et al., US Pub. No. 2004/0139352 as applied to claims 1, 15, 19, 22, 38, 52, 56, and 59 above, and further in view of Botz et al., US Pub. No. 2003/0177388.

As per claims 16 and 53:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 15 and 52. Not explicitly disclosed is wherein said secure channel comprises a network connection secured via the SSL (secure sockets layer) protocol. However, Botz et al. teach the use of SSL in a step to provide an initial authentication step. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to use a secure channel, such as SSL, in

order to ensure that the channel that the authentication information is being transmitted over is secure. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Botz et al. suggest (and as is commonly known in the art) that using SSL to provide a secure channel is necessary when authentication information is being transmitted from one entity to another in par. 31.

As per claims 19 and 56:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 1 and 38. Not explicitly disclosed is wherein said step of transmitting said stored, issued trust token occurs via a secured channel. However, Botz et al. teach the use of SSL in a step to provide an initial authentication step. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to use a secure channel, such as SSL, in order to ensure that the channel that the authentication information is being transmitted over is secure. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Botz et al. suggest (and as is commonly known in the art) that using SSL to provide a secure channel is necessary when authentication information is being transmitted from one entity to another in par. 31.

As per claims 20 and 57:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 19 and 56. Furthermore, Botz et al. teach wherein said secured channel comprises a network connection secured via the SSL (secure

sockets layer) protocol (par. 31).

As per claims 24 and 61:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 22 and 59. Not explicitly disclosed is wherein said secure channel comprising a network connection secured via the SSL (secure sockets layer) protocol. However, Botz et al. teach the use of SSL in a step to provide an initial authentication step. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to use a secure channel, such as SSL, in order to ensure that the channel that the authentication information is being transmitted over is secure. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Botz et al. suggest (and as is commonly known in the art) that using SSL to provide a secure channel is necessary when authentication information is being transmitted from one entity to another in par. 31.

VI. Claims 30-33, 36, 67-70, and 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crane et al., US Patent No., 6,510,236 and Shewchuk et al., US Pub. No. 2004/0139352 as applied to claims 1-2 and 39-40 above, and further in view of Malan, US Pub. No. 2002/0032793.

As per claims 30 and 67:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 1 and 39. Not explicitly disclosed is wherein processing remaining requests according to at least a second policy comprises adding a specified

amount of incremental response latency when processing untrusted logins. However, Malan et al. teach that if untrusted/malicious use of the network resources is detected, that particular connection may be subjected to a cut-back on the connection rate (par. 69). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Okamoto et al. to add incremental response latency if an untrusted login has been detected. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Malan et al. suggest that when malicious activity is detected an important measure in preventing an attack is to contain the amount of damages that may be incurred in par. 67-68.

As per claims 31 and 68:

Crane et al., Shewchuk et al., and Malan et al. substantially teach the method/computer program product on a computer readable medium of claims 30 and 67. Furthermore, Malan et al. teach wherein untrusted logins include successful and unsuccessful logins from entities not bearing a trust token (par. 75).

As per claim 32:

Crane et al., Shewchuk et al., and Malan et al. substantially teach the method of claim 31. Furthermore, Malan et al. teach wherein response latency is added to a configurable percentage of successful untrusted logins (par. 74-75).

As per claims 33 and 70:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 2 and 40. Not explicitly disclosed is wherein processing remaining requests according to at least a second policy comprises adding a specified

amount of incremental response latency when processing requests from untrusted IP addresses that have exceeded a configurable login rate. However, Malan et al. teach that if untrusted/malicious use of the network resources is detected based on malicious activity on a connection, that particular connection may be subjected to a cut-back on the connection rate (par. 69-70). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Okamoto et al. to add incremental response latency if an untrusted login has been detected. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Malan et al. suggest that when malicious activity is detected an important measure in preventing an attack is to contain the amount of damages that may be incurred in par. 67-68.

As per claims 36 and 73:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 35 and 72. Not explicitly disclosed is wherein said server applies rate policies for a plurality of network devices. However, Malan et al. teach that if untrusted/malicious use of the network resources is detected based on malicious activity on a connection by any client device, that particular connection may be subjected to a cut-back on the connection rate (par. 69-70). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Okamoto et al. to add incremental response latency if an untrusted login has been detected. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Malan et al. suggest that when malicious

activity is detected an important measure in preventing an attack is to contain the amount of damages that may be incurred in par. 67-68.

As per claim 69:

Crane et al. and Shewchuk et al. substantially teach the computer program product on a computer readable medium of claim 68. Not explicitly disclosed is wherein response latency is added to a specified percentage of successful logins. However, Malan et al. teach that if malicious use of the network resources is detected based on malicious activity on a connection (regardless of whether or not the entity is trusted), that particular connection may be subjected to a cut-back on the connection rate (par. 69-70). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Okamoto et al. to add incremental response latency if an untrusted login has been detected. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Malan et al. suggest that when malicious activity is detected an important measure in preventing an attack is to contain the amount of damages that may be incurred in par. 67-68.

VII. Claims 34 and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crane et al., US Patent No., 6,510,236 and Shewchuk et al., US Pub. No. 2004/0139352 as applied to claims 2 and 40 above, and further in view of Card, US Pub. No. 2002/0073339.

As per claims 34 and 71:

Crane et al. and Shewchuk et al. substantially teach the method/computer program product on a computer readable medium of claims 2 and 40. Not explicitly disclosed is wherein processing remaining requests according to at least a second policy comprises requiring an

untrusted entity to complete a Turing test. However, Card teaches that questioning the user based on information that only the user would know allows for stronger authentication. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to subject an untrusted entity to complete a Turing test in order to determine whether or not that user is a valid user or if the user should remain untrusted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Card suggests that requiring the user to answer a security question, which is known only to that user, in order to establish whether or not he/she should be trusted allows for stronger authentication in par. 43.

VIII. Claims 75-84, 89-91, and 93-94 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al., US Patent No. 5,944,794 and further in view of Malan, US Pub. No. 2002/0032793.

As per claim 75:

Okamoto et al. teach a method of establishing an entity requesting a network service as trusted, comprising the steps of: for each successful authentication, adding or updating a database record containing at least a user identifier, an originating network address and a date/timestamp of first and/or the current successful authentication (col. 13, line 55 - col. 14, line 3); comparing all subsequent authentication requests to said record; and where the user identifier of a subsequent request matches that of a successful authentication, extending trust to the subsequent request if its originating network address satisfy predetermined criteria in relation to said record (col. 14, lines 46-57 and col. 15, line 60 - col. 16, line 4); and processing request from trusted entities according to a first policy (col. 10, lines 61-64).

Not explicitly disclosed is processing remaining requests according to at least a second policy, wherein processing remaining requests according to at least the second policy comprises adding a configurable amount of incremental response latency when processing untrusted logins. However, Malan et al. teach that if untrusted/malicious use of the network resources is detected, that particular connection may be subjected to a cut-back on the connection rate (par. 69). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Okamoto et al. to add incremental response latency if an untrusted login has been detected. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Malan et al. suggest that when malicious activity is detected an important measure in preventing an attack is to contain the amount of damages that may be incurred in par. 67-68.

As per claim 76:

Okamoto et al. and Malan et al. substantially teach the method of claim 75. Furthermore, Okamoto et al. teach wherein said step of adding or updating a database record comprises either of the steps of: creating a new record by said network service if an entity has not previously authenticated to said network service (par. 46); and updating a previously created record for subsequent authentication requests from said entity (col. 9, line 63 - col. 10, line 8).

As per claim 77:

Okamoto et al. and Malan et al. substantially teach the method of claim 75. Okamoto et al. further teach wherein the network address comprises an IP (internet protocol) address (col. 15, lines 60-67).

As per claim 78:

Okamoto et al. and Malan et al. substantially teach the method of claim 75. Furthermore, Okamoto et al. teach wherein the step of extending trust to the subsequent request comprises: extending trust if the user identification and originating network address match those of the record exactly, and wherein the data/timestamps from the record satisfy specified bounds checks (col. 15, lines 60-67).

As per claim 79:

Okamoto et al. and Malan et al. substantially teach the method of claim 75. Furthermore, Okamoto et al. teach wherein the step of extending trust to the subsequent request comprises: when the user identifier of the subsequent request matches that of a record, determining a trusted address range, defined by client addresses from which successful authentications have originated, for the user identifier from stored authentication records (col. 11, line 60 - col. 12, line 15).

As per claim 80:

Okamoto et al. and Malan et al. substantially teach the method of claim 79. Furthermore, Okamoto et al. teach wherein the step of extending trust to the subsequent request further comprises: determining if the originating address of the subsequent request falls within the trusted address range (col. 12, lines 31-67), and determining if the data/timestamps for the trusted address range satisfy specified bounds checks (col. 13, lines 3-7).

As per claim 81:

Okamoto et al. and Malan et al. substantially teach the method of claim 79. Furthermore, Okamoto et al. teach wherein the step of determining if the data/timestamps for the trusted address range satisfy configurable bounds checks comprises the steps of: establishing earliest

date/timestamp for the trusted address range as a minimum for the earliest authentication timestamp; and establishing earliest date/timestamp for the trusted address range as a maximum for the earliest authentication timestamp (col. 13, lines 3-13 and col. 14, lines 3-37).

As per claim 82:

Okamoto et al. and Malan et al. substantially teach the method of claim 79. Furthermore, Okamoto et al. teach wherein the step of extending trust to the subsequent request further comprises: if the timestamps pass specified bounds checks, extending trust to the request (col. 15, lines 1-8).

As per claim 83:

Okamoto et al. and Malan et al. substantially teach the method of claim 75. Furthermore, Malan et al. teach wherein the entity comprises a user requesting the network service from an anonymous client (par. 116).

As per claim 84:

Okamoto et al. and Malan et al. substantially teach the method of claim 83. Furthermore, Okamoto et al. teach wherein the network service comprises a server (col. 8, lines 10-24).

As per claim 89:

Okamoto et al. and Malan et al. substantially teach the method of claim 75. Furthermore, Malan et al. teach wherein untrusted logins include successful and unsuccessful logins from untrusted entities (par. 75).

As per claim 90:

Okamoto et al. and Malan et al. substantially teach the method of claim 89. Furthermore, Malan et al. teach wherein response latency is added to a configurable percentage of successful untrusted logins (par. 74-75).

As per claim 91:

Okamoto et al. and Malan et al. substantially teach the method of claim 75. Furthermore, Malan et al. teach wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing requests from IP addresses that have exceeded a configurable login rate (par. 69-70).

As per claim 93:

Okamoto et al. and Malan et al. substantially teach the method of claim 75. Furthermore, Okamoto et al. teach wherein said policies are applied by a server (col. 8, lines 10-24).

As per claim 94:

Okamoto et al. and Malan et al. substantially teach the method of claim 91. Furthermore, Malan et al. teach wherein said server applies rate policies for a plurality of network devices (par. 69 and par. 75).

IX. Claims 85-86 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al., US Patent No. 5,944,794 and Malan, US Pub. No. 2002/0032793, as applied to claim 75 above, and further in view of Botz et al., US Pub. No. 2003/0177388.

As per claim 85:

Okamoto et al. and Malan et al. substantially teach the method of claim 84. Not explicitly disclosed is wherein the client and the server are in communication via a secured network channel. However, Botz et al. teach the use of SSL in a step to provide an initial

authentication step. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Crane et al. to use a secure channel, such as SSL, in order to ensure that the channel that the authentication information is being transmitted over is secure. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Botz et al. suggest (and as is commonly known in the art) that using SSL to provide a secure channel is necessary when authentication information is being transmitted from one entity to another in par. 31.

As per claim 86:

Okamoto et al., Malan et al., and Botz et al. substantially teach the method of claim 85. Furthermore, Botz et al. teach said secure channel comprising a network connection secured via the SSL (secure sockets layer) protocol (par. 31).

X. Claim 92 is rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al., US Patent No. 5,944,794 and Malan, US Pub. No. 2002/0032793, as applied to claim 75 above, and further in view of Card, US Pub. No. 2002/0073339.

As per claim 92:

Okamoto et al. and Malan et al. substantially teach the method of claim 87, wherein processing remaining requests according to at least a second policy comprises requiring an untrusted entity to complete a Turing test. However, Card teaches that questioning the user based on information that only the user would know allows for stronger authentication. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Okamoto et al. (as modified with Malan et al.) to subject an

untrusted entity to complete a Turing test in order to determine whether or not that user is a valid user or if the user should remain untrusted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Card suggests that requiring the user to answer a security question, which is known only to that user, in order to establish whether or not he/she should be trusted allows for stronger authentication in par. 43.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
10/10/2008

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437